Amendments to the Specification:

For the paragraph at page 7, lines 5 - 11 please amend as follows:

Let $f(x,y)$, $a(x,y)$, and $H(\xi,\eta)$ denote an image to be encrypted, an input random phase mask, and a Fourier random phase mask, respectively. The input random phase mask, $a(x,y)$, is bonded with the image $f(x, y)$. The resultant product of the two images is Fourier transformed and is multiplied by the Fourier phase mask $H(\xi,\eta)$. A second Fourier transform ~~products~~ produces the encrypted data. The encrypted data is recorded as a Fourier hologram, using an interference with the reference wave $R(\xi,\eta)$. The hologram $I_E(\xi,\eta)$ can be written as

For the paragraph at page 14, lines 12 - 14, please amend as follows:

Figure 17 shows the digitally reconstructed images that have been decrypted by inverse Fourier transforming the hologram of the encrypted data of Fig. 15A with hologram of the Fourier phase mask of Fig. 15B.

For the paragraph at page 14, line 16 - page 15, line 4, amend as follows:

In Figure 1 a schematic representation of a system for security verification is shown generally at 700. In particular in Figure 1 a source of coherent light 100 is provided to illuminate 102 first and second Fourier transform optical subsystems 200, 300, by way of mirrors 102a and beam splitter 104. The first Fourier transform optical subsystem 200 provides as output therefrom a first optical output signal 206 indicative of the Fourier transform of the convolution of the random code, $c(x,y)$, and the phase encoded primary image, $\exp\{i\pi f(x,y)/Max[f(x,y)]\}$. The second Fourier transform optical subsystem 300 provides as output therefrom a second optical output signal 312 indicative

of the Fourier transform of the a phase only convolved image, (x',y'). The first and second optical output signals 206, 312 are detected at a detector 400. A signal 402 indicative of the joint power spectrum of the first and second optical signals 206, 312 is

provided as output from the detector 400 to a verification subsystem 500 for correlation thereof.

For the paragraph at page 15, line 5 - page 16, line 4, please amend as follows:

The optical setup for security verification 700 is shown in Figure 1A as a nonlinear joint transform correlator (JTC) 700. The optical system 700 consists of two arms. In one arm, the convolution of a secondary image such as the phase encoded primary pattern $exp\{i\pi f(x,y)/Max[f(x,y)]\}$ and the random code, $c(x,y)$, is performed by use of a spatial filter matched to the random code $c(x,y)$, and positioned in the Fourier, or (u,v) plane. Light 102 is projected by beam expander 202 and collimating lens 204 at a spatial light modulator (SLM) 208. The phase-encoded primary pattern is displayed by means of thea spatial light modulator (SLM) 208. Fourier transform lens L_1 210, images the Fourier transform (FT) of the phase-encoded primary pattern, $F(u,v)$, in the Fourier, or (u,v), plane. The processor 700 has an *a-priori* knowledge of the random code mask $c(x,y)$. Thus, in the (u,v)-plane, a filter 212 with transmission $C(u,v)$ is placed. $C(u,v)$ is the Fourier transform of the random code $c(x,y)$. Lenses L_2 and L_3 (214, 216), image the complex amplitude distribution, formed at the filter plane, onto the (α,β)-plane, where a detector 400 is placed. Thus the Fourier transform of the convolution between the two functions $exp[i\,\pi f(x,y)/Max[f(x,y)]]$ and $c(x,y)$ is obtained in (α,β)-plane. In the other arm, an object, whose authenticity is to be verified and including a reference image such as the phase only distribution, (x',y'), is placed in the input plane (x',y') of the processor 700. Light 102 is projected by beam expander 314 and collimating lens 302 at 316 to a beam splitter 304. Coherent light 308 from the beam splitter 304 illuminates the reference image 602 from a card 600. Lens L_4 306 images (at 310) the Fourier transform of (x',y') onto the (α,β)-plane of the detector 400. Thus, a joint power spectrum is obtained in (α,β)-plane. The joint transform interference intensity is recorded by the detector 400 and is nonlinearly transformed by a nonlinear threshold function generator

502 in the verification subsystem 500. The resulting modified joint transform spectrum 504 is inverse Fourier transformed 506 and the modulus thereof squared to obtain the correlation at 508 of the primary image and the reference image. The correlation signal 512 may be obtained at 510 either by performing optical Fourier transform by displaying the modified intensity distribution written on the SLM, or by using discrete Fourier transform.

For the paragraph at page 17, line 9 - page 18, line 3, please amend as follows:

In addition, the robustness of the proposed optical security system in the presence of additive input noise is investigated. In the noise performance tests of the system, both white and colored noise are considered. The performance of the proposed method is investigated using a number of metrics. The signal to noise ratio, SNR, is defined as the ratio of the expected value squared of the correlation peak amplitude to the variance of the correlation peak amplitude. And the peak-to-output energy ~~ration~~ ratio metric, POE, is defined as the ratio of the expected value squared of the correlation peak to the average expected value of the output signal energy.

For the paragraph at page 18, lines 4 - 20, please amend as follows:

Throughout the simulations, fingerprint biometrics are used as the primary image; however the other biometrics can be used as well. The optical processor 700 was first tested for authenticity of a card encoded with a fingerprint information convolved with a random code in the absence of input noise and distortions. Two fingerprints are selected for computer simulation as shown in Figures 2A and 2B. The fingerprint in Figure 2A is chosen as authentic and the fingerprint in Figure 2B is considered as an unauthorized biometric image to be rejected. Figure 3A is the output correlation intensity for the authentic card, when the authorized fingerprint and code are used: A sharp and strong output peak for the authentic card is obtained. The simulations in Figures 3A-D were performed with nonlinearity index of $k = 0.3$ for the correlator. In the experiments, the correlation output are normalized by the maximum correlation peak obtained by the

authentic card. Figures 3 B, 3C and 3D show the output correlation intensity for the false-class input for which low level cross-correlations appear. Figure 3B shows the output correlations for an authorized fingerprint and an unauthorized random code. Figure 3C shows the correlation outputs for the authorized random code and an unauthorized fingerprint. Figure 3D shows the output correlation planes for an unauthorized fingerprint and an unauthorized code.

For the paragraph at page 20, line 25 - page 21 line 5, please amend as follows:

The robustness to missing data during the acquisition of the primary pattern information is tested. Figure 7 shows an example of input primary pattern with missing data when 25% of the authorized fingerprint is blocked. The results of the tests with missing input data are presented in Figures 8A-D. In the simulation presented here, additive white noise is used for both the input primary pattern (with a standard deviation equal to 0.3) and for the reference encoded on the credit card (with a standard deviation equal to 0.7).

For the paragraph at page 21, line 20 - page 22, line 17, please amend as follows:

The rotation-invariant pattern encoded on the card is given by the following equation,

$$\bar{p}(x,y) = \frac{\left\{\sum_a \exp\left[i\pi\ f_a(x,y) / \mathrm{Max}(f_a(x,y))\right]\right\} \otimes\ c(x,y)}{\left|\left\{\sum_a \exp\left[i\pi\ f_a(x,y) / \mathrm{Max}(f_a(x,y))\right]\right\} \otimes\ c(x,y)\right|} \qquad (14)$$

where $f_a(x,y)$ is the primary pattern rotated by an angle α. In the experiment presented here the sum is over -10 to +10 degrees in increments of 1 degree, and the rotation axis coincides with the center of the image. The correlation results correspond to nonlinear JTC for $k = 0.3$. Figure 9A is the output correlation intensity for the authentic input card, using a rotation-invariant reference image encoded on the card. Here the correct fingerprint is rotated by 7 degrees and the authorized code is used. A sharp and strong output peak is obtained, Figures 9B, 9C and 9D show the output correlation intensity for false inputs, where no correlation peak appears. In the simulation presented here, additive white noise is taken into account for both ~~forth~~ the input primary pattern (with a standard deviation equal to 0.3) and for the reference encoded on the card (with a standard deviation equal to 0.7). In the experiments, the correlation output is normalized by the maximum correlation peak obtained by the authentic card. Figure 9B shows the correlation output for an authorized random code and an unauthorized fingerprint. Figure 9C shows the output correlation for an authorized fingerprint and an unauthorized random code. Figure 9D shows the output correlation plane for an unauthorized fingerprint and an unauthorized code. The tests illustrate that the rotation invariant reference image provides tolerances to rotation of input primary images.

For the paragraph at page 23, lines 8 - 12 please amend as follows:

Figures 12A and 12B show a secure image/video-storage/transmission system based upon the proposed holographic system. The image/video data 602 are encrypted optically 604 to provide encrypted data 606 by the double-random phase encryption technique and recorded as a digital hologram 608. The optical key 610, that is, the Fourier phase mask, can also be recorded as a digital hologram. The encrypted data 606 can be decrypted digitally (system 702) with the hologram of the optical key 706 to provide image/video 704.

For the paragraph at page 23, lines 13 - 22, please amend as follows:

Referring to Figure 13, a Mach-Zehnder interferometer is shown generally at 800. A Helium-Neon laser 802 with a Spatial Filter (SF) 822 are ~~is~~ used a source of ~~used as a~~ coherent light ~~source~~ 844 which is collimated by collimating lens (CL) 824, split by beam

splitter (BS1) 832, and directed by mirror (M1) 828 to the arms. The lower arm 804 of the interferometer 800 is the optical path of the image encryption. The upper arm 806 is the reference wave. The input image to be encrypted is bonded with the input phase mask at plane P_1 (808). This product is transformed by lens L_1 (810). Such transformation may be for example a Fourier transformation or a Fresnel transformation. The transformation is multiplied by the Fourier phase mask at plane P_2 (812) and imaged onto the CCD camera by the 4-*f* optical system of lenses L_2 (814) and L_3 (816). The reference wave 838 passes through the 4-*f* optical system of lenses L_4 (818) and L_5 (820) to maintain the spatial coherence.

For the paragraph at page 23, line 23 - page 24, line 2, please amend as follows:

At the CCD camera 840, a hologram is created by the interference between the encrypted data and the slightly inclined reference plane wave 842 directed by mirror (M2) 826 and beam combiner (BS2) 834. The hologram 836 captured by the CCD 840 camera is sampled with 512 X 480 pixels and is quantized to 8 bits of gray levels by a frame-grabber board (not shown) to provide signal 848. The input image, the input phase mask, and the lens L_1 (810) are removed when we record the hologram of the Fourier phase mask. In the experiments, a random phase mask is used with a correlation length of less than 10μm as an input phase mask and a lens as the Fourier phase mask.

For the paragraph at page 24, lines 15 - 25, please amend as follows:

Digital holograms of the encrypted data and the Fourier phase mask are shown in Figures15A and 15B respectively. The digitally reconstructed encrypted images are shown in Figure 16. These images were obtained by inverse Fourier transforming of the digital hologram of the encrypted data. The original images cannot be recognized. The mean-square errors between the original images "MEMORY" and "UCONN" of Figure 14 and the encrypted images of Figures 15A and 15B are 7.3 and 6.6, respectively. The digitally reconstructed images that have been decrypted with the hologram of the Fourier phase mask are shown in Figure 17. The original images can be seen. The mean-square errors between the original images "MEMORY" and "UCONN" of Figure 14 and the

decrypted images of Figure 17 are 0.97 and 1.1, respectively. The experimental results demonstrate the feasibility of the proposed method.